McAfee

virusscan®

Guia do Usuário

COPYRIGHT

Copyright © 2005 McAfee, Inc. Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzida, transmitida, transcrita, armazenada em um sistema de recuperação ou traduzida para qualquer idioma, de qualquer forma ou por qualquer meio sem a permissão, por escrito, da McAfee Inc., seus fornecedores ou empresas associadas.

ATRIBUIÇÕES DE MARCAS COMERCIAIS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (E EM KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE E DESIGN, CLEAN-UP, DESIGN (E ESTILIZADO), DESIGN (N ESTILIZADO), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (E EM KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (E EM KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M E DESIGN, MCAFEE, MCAFEE (E EM KATAKANA), MCAFEE E DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (E EM KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (E EM KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (E EM KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS são marcas comerciais ou marcas registradas da McAfee, Inc. e/ou de suas empresas associadas nos EUA e/ou em outros países. O vermelho em relação à segurança é característica dos produtos da marca McAfee. Todas as outras marcas registradas e não registradas contidas neste documento são de propriedade exclusiva de seus respectivos proprietários.

INFORMAÇÕES SOBRE A LICENÇA

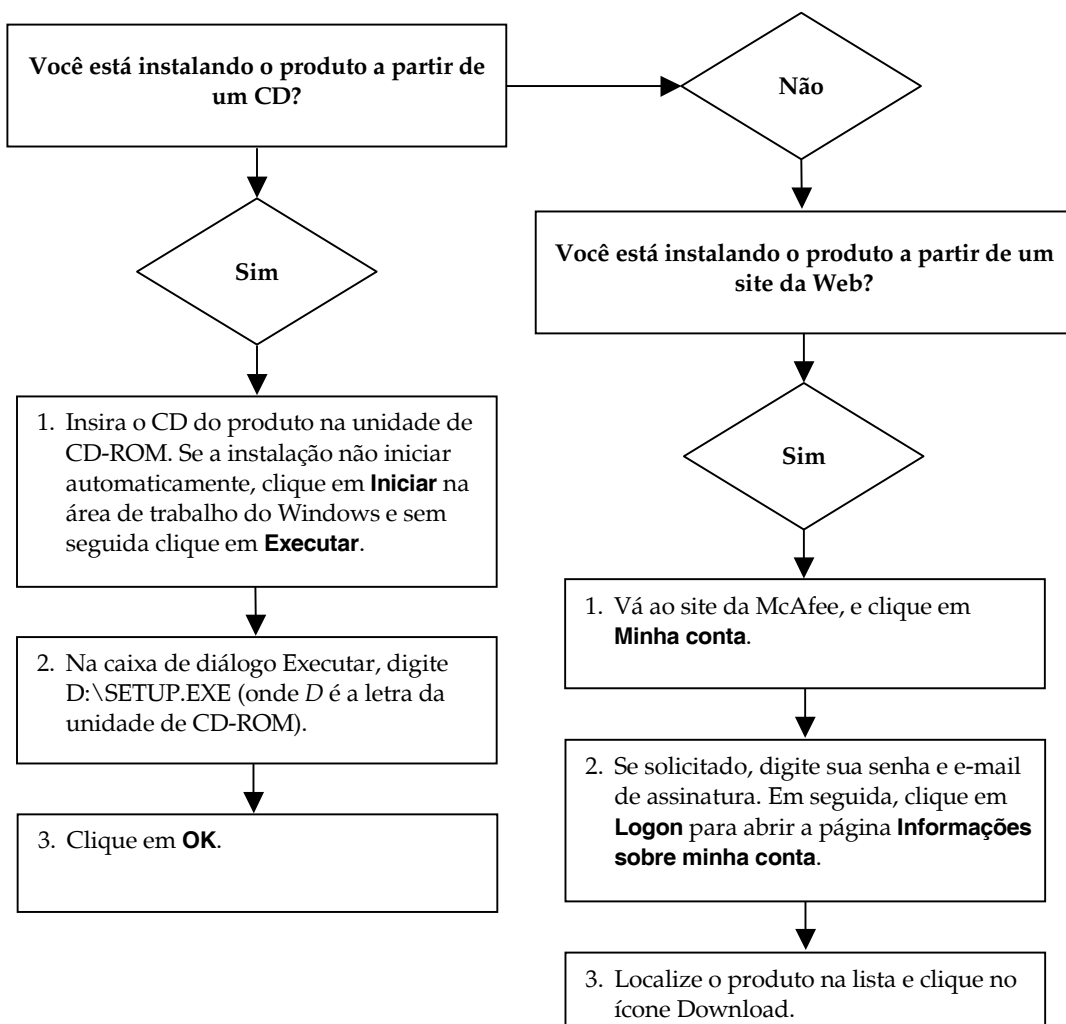
Contrato de licença

AVISO A TODOS OS USUÁRIOS: LEIA ATENTAMENTE O CONTRATO LEGAL CORRESPONDENTE À LICENÇA ADQUIRIDA POR VOCÊ. NELE ESTÃO DEFINIDOS OS TERMOS E AS CONDIÇÕES GERAIS PARA A UTILIZAÇÃO DO SOFTWARE LICENCIADO. CASO NÃO SAIBA O TIPO DE LICENÇA QUE VOCÊ ADQUIRIU, CONSULTE A DOCUMENTAÇÃO RELACIONADA À COMPRA E VENDA OU À CONCESSÃO DE LICENÇA, INCLUÍDA NO PACOTE DO SOFTWARE OU FORNECIDA SEPARADAMENTE (COMO UM LIVRETO, UM ARQUIVO NO CD DO PRODUTO OU UM ARQUIVO DISPONÍVEL NO SITE EM QUE O PACOTE DE SOFTWARE FOI OBTIDO POR DOWNLOAD). SE NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS NO CONTRATO, NÃO INSTALE O SOFTWARE. SE FOR APLICÁVEL, VOCÊ PODE DEVOLVER O PRODUTO PARA A MCAFEE, INC. OU PARA O LOCAL ONDE ADQUIRIU O PRDUTO, A FIM DE OBTER O REEMBOLSO TOTAL.

Atribuições

Este produto inclui ou pode incluir:
♦ Software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (http://www.openssl.org/). ♦ Software de criptografia criado por Eric A. Young e software criado por Tim J. Hudson. ♦ Alguns programas de software que estão licenciados (ou sublicenciados) ao usuário de acordo com a GNU General Public License (GPL) ou com outras licenças de Software livre que, entre outros direitos, permitem que os usuários copiem, modifiquem ou redistribuam determinados programas, ou partes deles, e também tenham acesso ao código fonte. A GPL exige, para qualquer um desses softwares licenciados e distribuídos em formato binário executável, que o código fonte seja disponibilizado a esses usuários. Para todos os softwares licenciados segundo a GPL, o código fonte está disponível neste CD. Se alguma licença de Software livre exigir que a McAfee, Inc. conceda direitos de uso, de cópia ou de modificação de um programa de software mais abrangentes que os direitos concedidos neste acordo, estes últimos terão precedência sobre as restrições e os direitos mencionados neste documento. ♦ Software criado originalmente por Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software criado originalmente por Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software criado por Douglas W. Sauder. ♦ Software desenvolvido pela Apache Software Foundation (http://www.apache.org/). Uma cópia do contrato de licença deste software pode ser encontrada em www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation e outros. ♦ Software desenvolvido pela CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Tecnologia Optimizer®, copyright Netopsystems AG, Berlim, Alemanha. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. e/ou Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software com copyright da Thai Open Source Software Center Ltd. e Clark Cooper, © 1998, 1999, 2000. ♦ Software com copyright dos mantenedores da Expat. ♦ Software com copyright da The Regents of the University of California, © 1989. ♦ Software com copyright de Gunnar Ritter. ♦ Software com copyright da Sun Microsystems®, Inc.© 2003. ♦ Software com copyright de Gisle Aas. © 1995-2003. ♦ Software com copyright de Michael A. Chase, © 1999-2000. ♦ Software com copyright de Neil Winton, © 1995-1996. ♦ Software com copyright da RSA Data Security, Inc., © 1990-1992. ♦ Software com copyright de Sean M. Burke, © 1999, 2000. ♦ Software com copyright de Martijn Koster, © 1995. ♦ Software com copyright de Brad Appleton, © 1996-1999. ♦ Software com copyright de Michael G. Schwern, © 2001. ♦ Software com copyright de Graham Barr, © 1998. ♦ Software com copyright de Larry Wall e Clark Cooper, © 1998-2000. ♦ Software com copyright de Frodo Looijaard, © 1997. ♦ Software com copyright da Python Software Foundation, Copyright © 2001, 2002, 2003. Uma cópia do contrato de licença deste software pode ser encontrada em www.python.org. ♦ Software com copyright de Beman Dawes, © 1994-1999, 2002. ♦ Software criado por Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software com copyright de Simone Bordet e Marco Cravero, © 2002. ♦ Software com copyright de Stephen Purcell, © 2001. ♦ Software desenvolvido pela Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software com copyright da International Business Machines Corporation e outros, © 1995-2003. ♦ Software desenvolvido pela University of California, Berkeley e seus colaboradores. ♦ Software desenvolvido por Ralf S. Engelschall <rse@engelschall.com> para uso no projeto mod_ssl (http://www.modssl.org/). ♦ Software com copyright de Kevlin Henney, © 2000-2002. ♦ Software com copyright de Peter Dimov e Multi Media Ltd. © 2001, 2002. ♦ Software com copyright de David Abrahams, © 2001, 2002. Consulte http://www.boost.org/libs/bind/bind.html para obter a documentação. ♦ Software com copyright de Steve Cleary, Beman Dawes, Howard Hinnant e John Maddock, © 2000. ♦ Software com copyright de Boost.org, © 1999-2002. ♦ Software com copyright de Nicolai M. Josuttis, © 1999. ♦ Software com copyright de Jeremy Siek, © 1999-2001. ♦ Software com copyright de Daryle Walker, © 2001. ♦ Software com copyright de Chuck Allison e Jeremy Siek, © 2001, 2002. ♦ Software com copyright de Samuel Krempp, © 2001. Consulte http://www.boost.org para obter atualização, documentação e histórico da revisão. ♦ Software com copyright de Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software com copyright da Cadenza New Zealand Ltd., © 2000. ♦ Software com copyright de Jens Maurer, © 2000, 2001. ♦ Software com copyright de Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software com copyright de Ronald Garcia, © 2002. ♦ Software com copyright de David Abrahams, Jeremy Siek, e Daryle Walker, © 1999-2001. ♦ Software com copyright de Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software com copyright de Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software com copyright de Paul Moore, © 1999. ♦ Software com copyright de Dr. John Maddock, © 1998-2002. ♦ Software com copyright de Greg Colvin e Beman Dawes, © 1998, 1999. ♦ Software com copyright de Peter Dimov, © 2001, 2002. ♦ Software com copyright de Jeremy Siek e John R. Bandela, © 2001. ♦ Software com copyright de Joerg Walter e Mathias Koch, © 2000-2002.

Cartão de início rápido

Se você estiver instalando o produto de um CD ou de um site da Web, imprima esta página de referência.

A McAfee se reserva o direito de atualizar os planos e as diretivas de Atualização e Suporte a qualquer momento, sem aviso prévio. McAfee e os nomes de seus produtos são marcas registradas da McAfee, Inc. e/ou de suas empresas associadas nos EUA e/ou em outros países.
© 2005 McAfee, Inc. Todos os direitos reservados.

Para obter mais informações

Para ver os Guias do Usuário contidos no CD do produto, verifique se o Acrobat Reader está instalado. Se não estiver, instale-o agora com o CD do produto da McAfee.

1. Insira o CD do produto na unidade de CD-ROM.
2. Abra o Windows Explorer: Clique em **Iniciar** na área de trabalho do Windows e, em seguida, em **Pesquisar**.
3. Localize a pasta Manuais e clique duas vezes no arquivo .PDF do Guia do Usuário que você deseja abrir.

Benefícios do registro

A McAfee recomenda que você siga as etapas fáceis indicadas no produto para que o seu registro seja transmitido diretamente para nós. O registro garante que você receba assistência técnica adequada e confiável, e oferece também os seguintes benefícios:

- Suporte eletrônico GRATUITO.
- Atualizações de arquivos (.DAT) com definição dos vírus por um ano após a instalação quando você adquire o software VirusScan.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional das assinaturas de vírus.
- Garantia de 60 dias, que cobre a substituição do CD do software se ele apresentar defeito ou se estiver danificado.
- Atualização do filtro SpamKiller por um ano após a instalação quando você adquire o software SpamKiller.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional de atualizações do filtro.
- Atualização do pacote McAfee Internet Security por um ano após a instalação quando você adquire o software MIS.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional de atualizações do conteúdo.

Suporte técnico

Para obter suporte técnico, consulte http://www.mcafeehelp.com/.

Nosso site de suporte oferece acesso ininterrupto ao Assistente de Respostas de fácil utilização, que contém soluções para as questões de suporte mais comuns.

Os usuários mais experientes também podem experimentar as opções avançadas, que incluem uma pesquisa de palavra-chave e nossa árvore de ajuda. Se a solução não for encontrada, é possível acessar as opções GRATUITAS do Chat Now! e do E-mail Express! . O Chat e o e-mail ajudam a contatar os engenheiros de suporte qualificados de forma rápida pela Internet, sem custo nenhum. Como alternativa, é possível obter informações do suporte telefônico em http://www.mcafeehelp.com/.

Sumário

Introdução 1

Bem-vindo ao McAfee VirusScan.

O McAfee VirusScan é um serviço de assinatura antivírus que oferece proteção abrangente, confiável e atualizada contra vírus. Equipado com a premiada tecnologia de varredura da McAfee, o VirusScan protege o computador contra vírus, worms, cavalos de Tróia, scripts suspeitos, ataques híbridos e outras ameaças.

Ele oferece os seguintes recursos:

ActiveShield — faz a varredura dos arquivos quando eles são acessados por você ou pelo seu computador.

Fazer varredura — Procura vírus e outras ameaças em unidades de disco rígido, em disquetes e em arquivos e pastas individuais.

Quarentena — Criptografa e isola temporariamente os arquivos suspeitos na pasta de quarentena até que uma ação apropriada possa ser realizada.

Detecção de atividades hostis — Monitora o computador em busca de atividades semelhantes a vírus causadas por scripts suspeitos e atividades de worms.

Novos recursos

Esta versão do VirusScan possui os seguintes novos recursos:

- **Detecção e remoção de spyware e adware**
  O VirusScan identifica e remove spyware, adware e outros programas que comprometem a privacidade e reduzem o desempenho do computador.

- **Atualizações automáticas diárias**
  As atualizações automáticas diárias do VirusScan protegem contra as mais recentes ameaças ao computador, identificadas ou não.

- **Varredura rápida em segundo plano**
  Varreduras rápidas e discretas, que identificam e destroem vírus, cavalos de Tróia, worms, spyware, adware, discadores e outras ameaças sem interromper o seu trabalho.

- **Alertas de segurança em tempo real**
  Os alertas de segurança notificam sobre epidemias de vírus de emergência e ameaças à segurança. Também oferecem opções de resposta para remover, neutralizar ou aprender mais sobre a ameaça.

- **Detecção e limpeza em múltiplos pontos de entrada**
  O VirusScan monitora e limpa os principais pontos de entrada do computador: e-mails, anexos de mensagens instantâneas e downloads da Internet.

- **Monitoração de e-mail para atividades semelhantes a de worms**
  O WormStopper™ faz a monitoração de comportamentos suspeitos de envio de mensagens em massa e impede a disseminação de vírus e worms por e-mail em outros computadores.

- **Monitoração de script para atividades semelhantes a de worms**
  O ScriptStopper™ monitora a execução de scripts suspeitos e impede a disseminação de vírus e worms por e-mail em outros computadores.

- **Suporte técnico gratuito para e-mail e mensagens instantâneas**
  O suporte técnico ao vivo fornece assistência imediata e fácil, usando troca de mensagens instantâneas e e-mails.

Requisitos do sistema

- Microsoft® Windows 98, Windows Me, Windows 2000 ou Windows XP
- Computador com processador compatível com Pentium
  Windows 98, 2000: 133 MHz ou superior
  Windows Me: 150 MHz ou superior
  Windows XP (Home e Pro): 300 MHz ou superior
- RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home e Pro): 128 MB
- 40 MB de espaço em disco rígido
- Microsoft® Internet Explorer 5.5 ou posterior

NOTA
Para atualizar para a versão mais recente do Internet Explorer, visite o site da Microsoft em http://www.microsoft.com/.

Programas de e-mail suportados

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Programas de mensagens instantâneas suportados

- AOL Instant Messenger 2.1 ou posterior
- Yahoo Messenger 4.1 ou posterior
- Microsoft Windows Messenger 3.6 ou posterior
- MSN Messenger 6.0 ou posterior

Testando o VirusScan

Antes de começar a usar o VirusScan, deve-se testar a sua instalação. Siga as etapas a seguir para testar separadamente os recursos Fazer varredura e ActiveShield.

Testando o ActiveShield

NOTA
Para testar o ActiveShield a partir da guia VirusScan no SecurityCenter, clique em **Testar VirusScan** para ver uma seção de FAQ de suporte online que contenha essas etapas.

Para testar o ActiveShield:

1 Vá para http://www.eicar.com/ no seu navegador da web.

2 Clique no link **The AntiVirus testfile eicar.com**.

3 Vá para o final da página. Em **Download**, você verá quatro links.

4 Clique em **eicar.com**.

Se o ActiveShield estiver funcionando adequadamente, ele detectará o arquivo eicar.com imediatamente após o clique no link. Experimente excluir ou colocar em quarentena arquivos detectados para saber como o ActiveShield lida com possíveis ameaças. Consulte *Entendendo os alertas de segurança* na página 23 para obter detalhes.

Testando o mecanismo de varredura

Antes de testar o mecanismo de varredura, é necessário desativar o ActiveShield para impedir que ele detecte os arquivos de teste antes da varredura. Após desativá-lo, faça o download dos arquivos de teste.

Para fazer download dos arquivos de teste:

1 Desative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.

2 Faça o download de arquivos de teste EICAR no site da EICAR:

   a Vá para http://www.eicar.com/.

   b Clique no link **The AntiVirus testfile eicar.com**.

c Vá para o final da página. Em **Download**, você verá estes links.

eicar.com contém uma linha de texto que o VirusScan detectará como vírus.

eicar.com.txt (opcional) é o mesmo arquivo, mas com um outro nome, para os usuários que possuem dificuldade em fazer o download do primeiro link. Simplesmente renomeie o arquivo como “eicar.com” após o download.

O arquivo **eicar_com.zip** é uma cópia do vírus de teste em um arquivo .ZIP compactado (arquivo WinZip™).

O **eicarcom2.zip** é uma cópia do vírus de teste dentro de um arquivo compactado .ZIP que, por sua vez, está dentro de um arquivo compactado ZIP.

d Clique em cada link para fazer o download do arquivo correspondente. Para cada um, uma caixa de diálogo **Download de arquivo** será exibida.

e Clique em **Salvar**, clique no botão **Criar nova pasta** e renomeie a pasta como **Pasta de varredura de VSO**.

f Clique duas vezes em **Pasta de varredura de VSO** e, em seguida, clique em **Salvar** novamente em cada caixa de diálogo **Salvar como**.

3 Quando terminar o download dos arquivos, feche o Internet Explorer.

4 Ative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**.

Para testar a opção Fazer varredura:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.

2 Utilizando a árvore de diretório no painel esquerdo da caixa de diálogo, vá até a **Pasta de varredura de VSO** em que você salvou os arquivos:

a Clique no sinal de **+** ao lado do ícone da unidade C.

b Clique em **Pasta de varredura do VSO** para selecioná-la (não clique no sinal de **+** ao lado dessa opção).

Isso indica que a opção Fazer varredura deve verificar se há vírus apenas nessa pasta. Você também pode colocar os arquivos em locais aleatórios na unidade de disco rígido para obter uma demonstração mais convincente da capacidade do recurso Fazer varredura.

3 Na área **Opções de varredura** da caixa de diálogo **Fazer varredura**, verifique se todas as opções estão selecionadas.

4 Clique em **Fazer varredura** na parte inferior direita da caixa de diálogo.

O VirusScan examina a **Pasta de varredura de VSO**. Os arquivos de teste EICAR que você salvou nessa pasta serão exibidos na **Lista de arquivos detectados**. Isso significa que a varredura está funcionando adequadamente.

Experimente excluir ou colocar em quarentena os arquivos detectados para saber como o recurso Fazer varredura lida com possíveis ameaças. Consulte *Entendendo as detecções de ameaças* na página 32 para obter detalhes.

Usando o McAfee SecurityCenter

O McAfee SecurityCenter é a sua central de produtos de segurança, acessível a partir do ícone correspondente na bandeja de sistema do Windows ou na área de trabalho do Windows. Com ele, você pode executar as seguintes tarefas:

- Obter uma análise gratuita de segurança do seu computador.
- Iniciar, gerenciar e configurar todas as suas assinaturas da McAfee usando um único ícone.
- Exibir alertas de vírus continuamente atualizados e as informações mais recentes sobre os produtos.
- Obter links rápidos para perguntas freqüentes e detalhes da conta no site da McAfee.

NOTA
Para obter mais informações sobre seus recursos, clique em **Ajuda** na caixa de diálogo do **SecurityCenter**.

Enquanto o SecurityCenter estiver sendo executado e todos os recursos da McAfee instalados no computador estiverem ativados, um ícone M vermelho será exibido na bandeja de sistema do Windows. Geralmente, essa área se encontra no canto inferior direito da área de trabalho do Windows e contém o relógio.

Se um ou mais aplicativos da McAfee instalados no computador forem desativados, o ícone da McAfee se tornará preto .

Para abrir o McAfee SecurityCenter:

1 Clique com o botão direito do mouse no ícone da McAfee .

2 Clique em **Abrir o SecurityCenter**.

Para acessar um recurso do VirusScan:

1 Clique com o botão direito do mouse no ícone da McAfee .

2 Aponte para **VirusScan** e clique no recurso que deseja usar.

Usando o McAfee VirusScan 2

Usando o ActiveShield

Quando o ActiveShield é iniciado (carregado na memória do computador) e ativado, passa a proteger continuamente o seu computador. O ActiveShield faz a varredura dos arquivos quando eles são acessados por você ou pelo computador. Quando detecta um arquivo, o ActiveShield tenta limpá-lo automaticamente. Se o ActiveShield não puder limpar o vírus, coloque o arquivo em quarentena ou exclua-o.

Ativando ou desativando o ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado pelo M vermelho na bandeja de sistema do Windows) assim que o computador é reiniciado após o processo de instalação.

Se o ActiveShield estiver interrompido (não carregado) ou desativado (indicado pelo ícone em preto M), você poderá executá-lo manualmente e configurá-lo para que seja iniciado automaticamente junto com o Windows.

Ativando o ActiveShield

Para ativar o ActiveShield somente nesta sessão do Windows:

Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**. O ícone da McAfee será alterado para a cor vermelha M.

Se o ActiveShield ainda estiver configurado para iniciar com o Windows, uma mensagem informará que você está protegido contra ameaças. Caso contrário, será exibida uma caixa de diálogo em que você poderá configurar o ActiveShield para que seja iniciado junto com o Windows (Figura 2-1 na página 14).

Desativando o ActiveShield

Para desativar o ActiveShield somente para esta sessão do Windows:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.
2. Clique em **Sim** para confirmar.

   O ícone da McAfee será alterado para preto M.

Se o ActiveShield ainda estiver configurado para iniciar com o Windows, o computador estará protegido contra ameaças novamente quando for reiniciado.

Configurando as opções do ActiveShield

Você pode modificar as opções de inicialização e varredura do ActiveShield na guia **ActiveShield** a caixa de diálogo **Opções do VirusScan** (Figura 2-1), que pode ser acessada através do ícone da McAfee na bandeja de sistema do Windows.

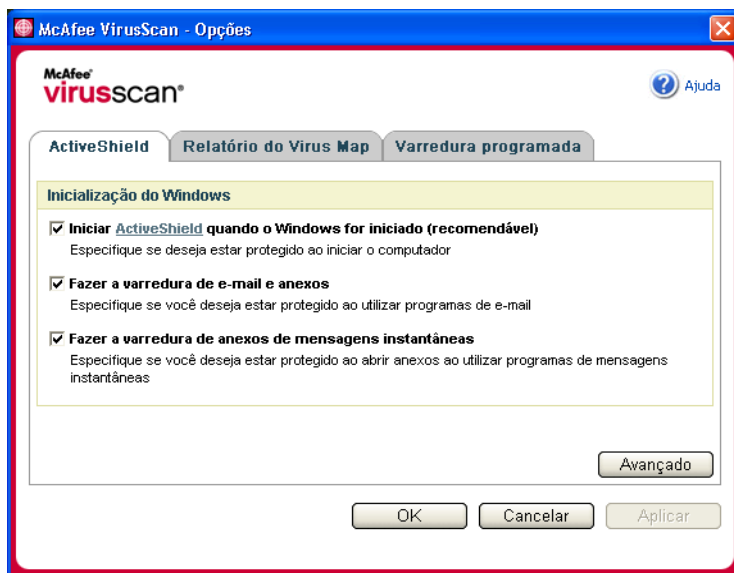



Figura 2-1. Opções do ActiveShield

Iniciando o ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado por um vermelho) assim que você reinicia o computador após o processo de instalação.

Se o ActiveShield for interrompido (representado por um preto), você poderá configurá-lo para que seja iniciado automaticamente junto com o Windows (recomendável).

NOTA
Durante a atualização do VirusScan, o **Assistente de atualização** pode sair do ActiveShield temporariamente para instalar arquivos novos. Quando o **Assistente de atualização** solicitar que você clique em **Concluir**, o ActiveShield será iniciado novamente.

Para inicializar o ActiveShield automaticamente junto com o Windows :

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta (Figura 2-1 na página 14).

2. Marque a caixa de seleção **Iniciar o ActiveShield quando o Windows for iniciado (recomendável)** e clique em **Aplicar** para salvar as alterações.

3. Clique em **OK** para confirmar e, em seguida, clique em **OK**.

Interrompendo o ActiveShield

AVISO
Se você interromper o ActiveShield, o seu computador não estará protegido contra ameaças. Se for necessário interromper o ActiveShield para outros fins que não seja a atualização do VirusScan, certifique-se de não estar conectado à Internet.

Para que o ActiveShield não seja iniciado junto com o Windows:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta (Figura 2-1 na página 14).

2. Desmarque a caixa de seleção **Iniciar o ActiveShield quando o Windows for iniciado (recomendável)** e clique em **Aplicar** para salvar as alterações.

3. Clique em **OK** para confirmar e, em seguida, clique em **OK**.

Fazendo a varredura de e-mails e anexos

Por padrão, a varredura de e-mail e a limpeza automática são ativadas na opção **Faze varredura de e-mail e de anexos** (Figura 2-1 na página 14).

Quando essa opção está ativada, o ActiveShield faz a varredura automaticamente e tenta limpar as mensagens e os anexos de e-mail detectados enviados (SMTP) e recebidos (POP3) pelos clientes de e-mail mais utilizados, incluindo os seguintes:

- Microsoft Outlook Express 4.0 ou posterior
- Microsoft Outlook 97 ou posterior
- Netscape Messenger 4.0 ou posterior
- Netscape Mail 6.0 ou posterior
- Eudora Light 3.0 ou posterior
- Eudora Pro 4.0 ou posterior
- Eudora 5.0 ou posterior
- Pegasus 4.0 ou posterior

NOTA
Não há suporte à varredura de e-mails nos seguintes clientes de e-mail: clientes baseados na Web, IMAP, AOL, POP3 SSL e Lotus Notes. No entanto, o ActiveShield faz a varredura de anexos de e-mail quando são abertos.

Se você desativar a opção **Fazer a varredura de e-mail e anexos**, as opções da varredura de e-mail e do WormStopper (Figura 2-2 na página 17) serão automaticamente desativadas. Quando a varredura de e-mails enviados é desativada, as opções do WormStopper são desativadas automaticamente.

Se você alterar as opções de varredura de e-mails, reinicie o programa de e-mail para efetuar essas alterações.

E-mails recebidos

Quando uma mensagem ou um anexo de e-mail recebido é detectado, o ActiveShield executa as seguintes etapas:

- Tenta limpar o e-mail detectado.
- Tenta colocar em quarentena ou excluir o e-mail que não pode ser limpo.
- Inclui um arquivo de alerta no e-mail recebido, contendo informações sobre as ações a serem executadas para remover a possível ameaça.

E-mails enviados

Quando uma mensagem ou um anexo de e-mail enviado é detectado, o ActiveShield executa as seguintes etapas:

- Tenta limpar o e-mail detectado.
- Tenta colocar em quarentena ou excluir o e-mail que não pode ser limpo.

NOTA
Para obter detalhes sobre os erros da varredura de e-mails enviados, consulte a ajuda online.

Desativando a varredura de e-mails

Por padrão, o ActiveShield faz a varredura de e-mails recebidos e enviados. Porém, para melhor controle, é possível configurar o ActiveShield para fazer a varredura somente de e-mails recebidos ou enviados.

Para desativar a varredura de e-mails recebidos ou enviados:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Varredura de e-mail** (Figura 2-2).
3. Desmarque **Mensagens de e-mail recebidas** ou **Mensagens de e-mail enviadas** e clique em **OK**.

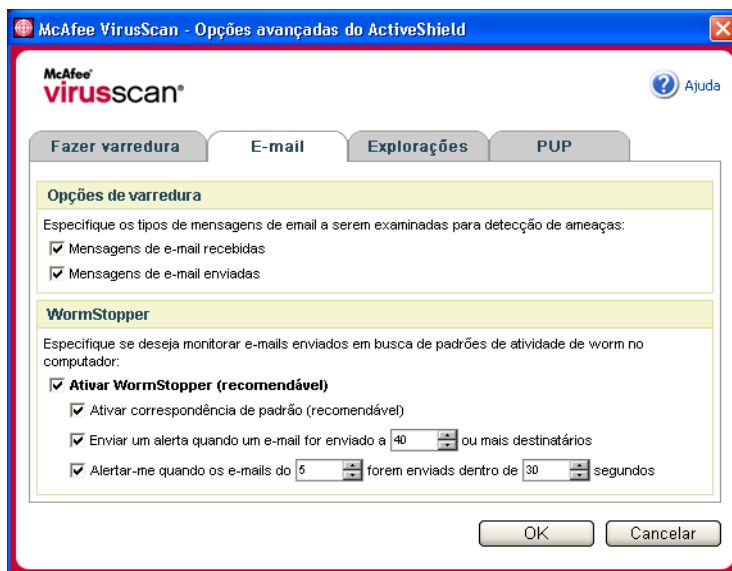



Figura 2-2. Opções avançadas do ActiveShield - Guia e-mail

Fazendo a varredura para worms

O VirusScan monitora o computador verificando atividades suspeitas que podem indicar a presença de ameaças. Enquanto o VirusScan limpa vírus e as outras ameaças, o WormStopper™ evita que vírus, worms e cavalos de Tróia se espalhem ainda mais.

Um "worm" de computador é um vírus que se replica automaticamente, reside na memória e pode enviar cópias de si mesmo por e-mail. Sem o WormStopper, os worms são percebidos apenas quando suas réplicas descontroladas consomem recursos do sistema, diminuindo o desempenho ou interrompendo tarefas.

O mecanismo de proteção do WormStopper detecta, alerta e bloqueia atividades suspeitas. As atividades suspeitas podem executar as seguintes ações no computador:

- Tentativas de encaminhar e-mails a muitos contatos da lista de endereços.
- Tentativas de encaminhar várias mensagens de e-mail em uma seqüência rápida

Se o ActiveShield for configurado para usar a opção padrão **Ativar WormStopper (recomendável)** da caixa de diálogo **Opções avançadas**, o WormStopper monitorará a atividade de e-mail em busca de padrões de atividades suspeitas e enviará um alerta quando o número especificado de e-mails ou de destinatários for excedido dentro de um determinado intervalo.

Para configurar o ActiveShield para fazer a varredura de mensagens de e-mail enviadas quanto a atividades semelhantes a worms:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **E-mail**.
3. Clique em **Ativar WormStopper (recomendável)** (Figura 2-3).

   Por padrão, as seguintes opções detalhadas estão ativadas:

   - Correspondência de padrões para detectar atividades suspeitas
   - Envio de alertas quando um e-mail é enviado a 40 ou mais destinatários
   - Envio de alertas quando 5 ou mais e-mails são enviados em 30 segundos

     NOTA
     Se você alterar o número de destinatários ou de segundos para a monitoração de e-mails enviados, poderão ocorrer detecções inválidas. A McAfee recomenda que você clique em **Não** para manter as configurações padrão. Se preferir, clique em **Sim** para alterar as configurações.

   Esta opção pode ser ativada automaticamente depois que um worm em potencial for detectado pela primeira vez (consulte os detalhes em *Gerenciando possíveis worms* na página 25):

   - Bloqueio automático de e-mails suspeitos enviados

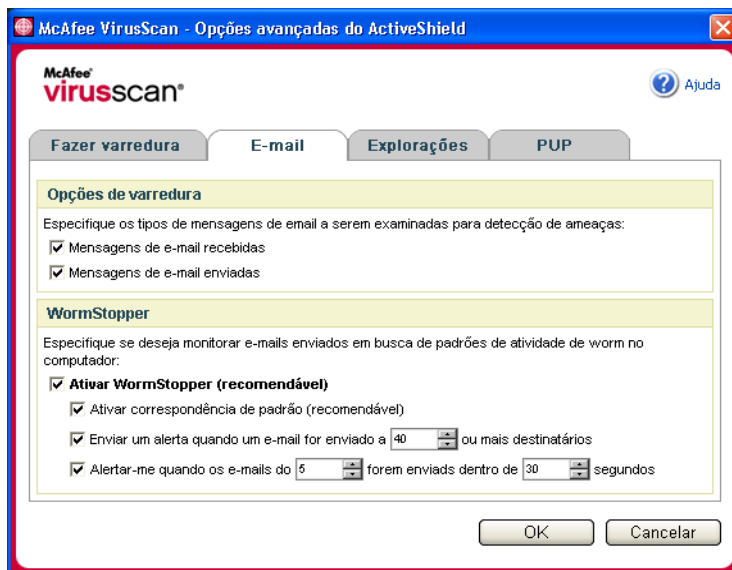



Figura 2-3. Guia Opções avançadas do ActiveShield - e-mail

Fazendo a varredura de anexos de mensagens instantâneas recebidas

Por padrão, a varredura de anexos de mensagens instantâneas é ativada através da opção **Fazer a varredura de anexos de mensagens instantâneas**. (Figura 2-1 na página 14).

Quando essa opção está ativada, o VirusScan faz a varredura automática e tenta limpar os anexos detectados de mensagens instantâneas recebidas dos programas de mensagens instantâneas mais utilizados, incluindo os seguintes:

- MSN Messenger 6.0 ou posterior
- Yahoo Messenger 4.1 ou posterior
- AOL Instant Messenger 2.1 ou posterior

NOTA
Para sua proteção, não é possível desativar a limpeza automática dos anexos de mensagens instantâneas.

Quando um anexo de mensagem instantânea recebida é detectado, o VirusScan executa as seguintes etapas:

- Tenta limpar a mensagem detectada.
- Pergunta se deve colocar em quarentena ou excluir a mensagem que não pode ser limpa.

Fazendo a varredura de todos os arquivos

Se você definir o ActiveShield para utilizar a opção padrão **Todos os arquivos (recomendável)**, ele fará a varredura de todos os tipos de arquivos no computador, à medida que este tenta utilizá-los. Utilize esta opção para obter a varredura mais completa possível.

Para configurar o ActiveShield para fazer a varredura de todos os tipos de arquivo:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura**. (Figura 2-4 na página 20).
3. Clique em **Todos os arquivos (recomendável)** e, em seguida, clique em **OK**.

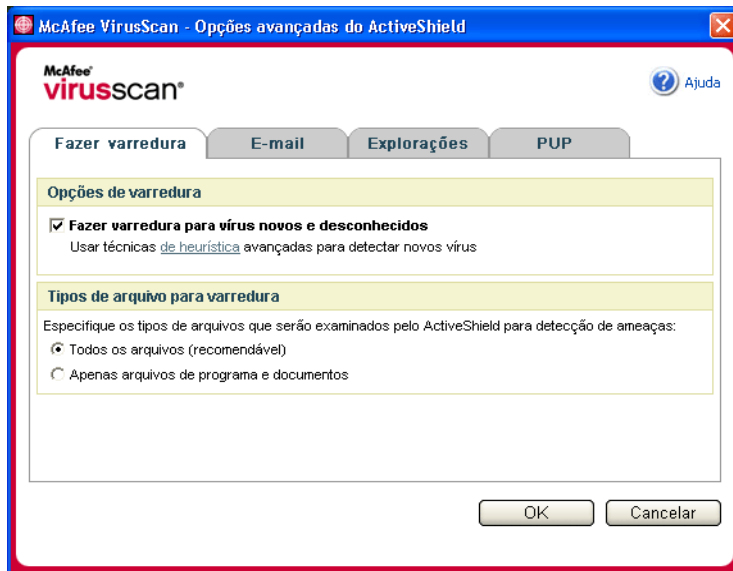



Figura 2-4. Opções avançadas do ActiveShield - Guia Fazer varredura

Fazendo a varredura somente de arquivos de programa e documentos

Se você definir o ActiveShield para utilizar a opção **Apenas arquivos de programa e documentos**, ele fará a varredura somente de documentos e arquivos de programas. O arquivo de assinatura de vírus mais recente (DAT determina quais tipos de arquivos serão examinados pelo ActiveShield. Para configurar o ActiveShield para fazer a varredura apenas de arquivos de programas e documentos:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

2 Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura**. (Figura 2-4).

3 Clique em **Somente arquivos de programa e documentos** e, em seguida, clique em **OK**.

Fazendo a varredura para vírus novos e desconhecidos

Se você definir o ActiveShield para utilizar a opção padrão **Fazer varredura para vírus novos e desconhecidos (recomendável)**, ela utiliza técnicas de heurística avançadas que tentam corresponder os arquivos às assinaturas de vírus conhecidos, ao mesmo tempo em que procura indícios de vírus desconhecidos nos arquivos.

Para configurar o ActiveShield para fazer a varredura de vírus novos e desconhecidos:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2 Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura**. (Figura 2-4).
3 Clique em **Fazer a varredura para vírus novos e desconhecidos (recomendável)** e, em seguida, clique em **OK**.

Fazendo a varredura para scripts

O VirusScan monitora o computador verificando atividades suspeitas que podem indicar a presença de ameaças. Enquanto o VirusScan limpa vírus e outras ameaças, o ScriptStopper™ evita que cavalos de Tróia executem os scripts que disseminam ainda mais os vírus.

Um “cavalo de Tróia” é um programa suspeito que finge ser um aplicativo benigno. Os cavalos de Tróia não são vírus porque não se replicam, mas podem ser tão destruidores quanto os vírus.

O mecanismo de proteção do ScriptStopper detecta, alerta e bloqueia atividades suspeitas. As atividades suspeitas podem incluir as seguintes ações no computador:

- Execução de scripts que resulte na criação, cópia ou exclusão de arquivos, ou na abertura do Registro do Windows.

Quando o ActiveShield é configurado para usar a opção padrão **Ativar ScriptStopper (recomendável)** da caixa de diálogo **Opções avançadas**, o ScriptStopper monitora a execução de scripts em busca de padrões suspeitos e envia alertas quando o número especificado de e-mails ou de destinatários foi excedido dentro de um determinado intervalo.

Para configurar o ActiveShield para fazer a varredura de scripts em execução cuja atividade seja semelhante à de worms:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2 Clique em **Avançado** e, em seguida, clique na guia **Explorações** (Figura 2-5).
3 Clique em **Ativar ScriptStopper (recomendável)** e, em seguida, clique em **OK**.

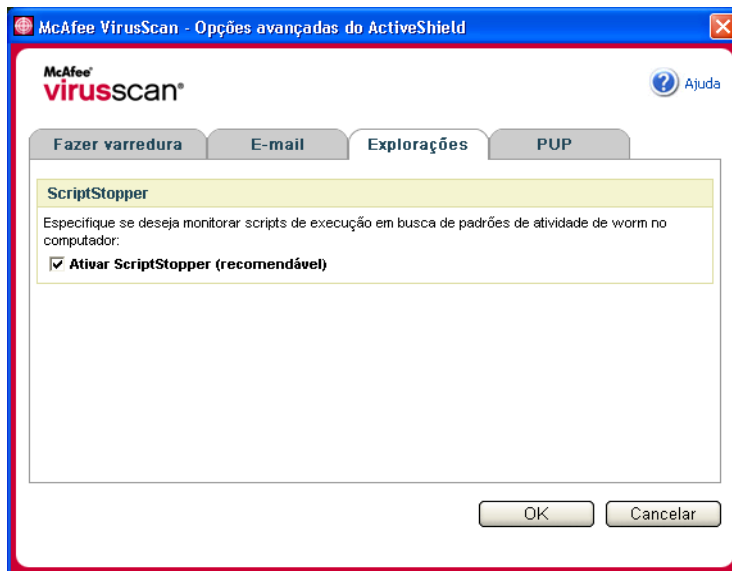



Figura 2-5. Opções avançadas do ActiveShield - Guia Explorações

Fazendo a varredura para Programas potencialmente indesejados (PUPs)

NOTA
Após ser instalado no computador, o McAfee AntiSpyware gerencia todas as atividades de programas potencialmente indesejados (PUPs). Abra o McAfee AntiSpyware para configurar as opções.

Se você definir o ActiveShield para utilizar a opção padrão **Fazer a varredura de programas potencialmente indesejados (recomendável)** na caixa de diálogo **Opções Avançadas**, a proteção contra programas potencialmente indesejados (PUP) detecta, bloqueia e remove rapidamente spyware, adware e outros programas que coletam e transmitem os seus dados particulares sem a sua permissão.

Para configurar o ActiveShield para fazer a varredura de PUPs:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

2 Clique em **Avançado** e, em seguida, clique na guia **PUPs** (Figura 2-6).

3 Clique em **Fazer a varredura de programas potencialmente indesejados (recomendável)** e, em seguida, clique em **OK**.

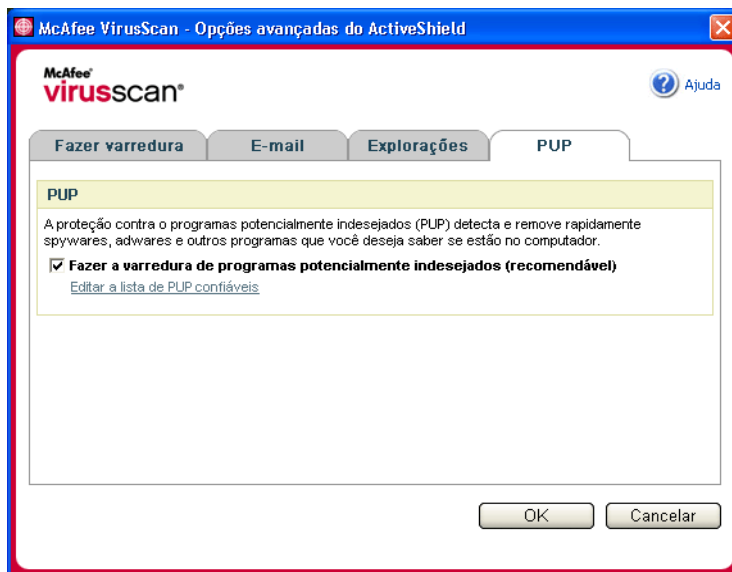



Figura 2-6. Opções avançadas do ActiveShield - Guia PUPs

Entendendo os alertas de segurança

Se o ActiveShield localizar um vírus, um alerta de vírus semelhante a Figura 2-7 será exibido. Para a maioria dos vírus, cavalos de Tróia, e worms, o ActiveShield tenta automaticamente limpar o arquivo e enviar um alerta para você. Para programas potencialmente indesejados (PUPs), o ActiveShield detecta o arquivo, bloqueia-o automaticamente e envia um alerta a você.

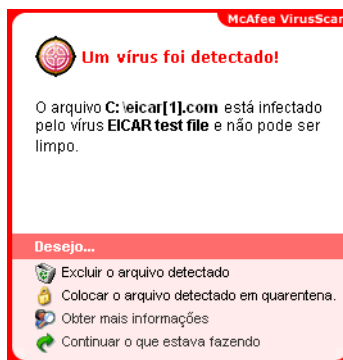



Figura 2-7. Alerta de vírus

Você pode escolher como gerenciar arquivos detectados, e-mails detectados, scripts suspeitos, worms potenciais ou PUPs e se deseja enviar os arquivos detectados aos laboratórios AVERT da McAfee para que sejam pesquisados.

Para maior proteção, sempre que o ActiveShield detecta um arquivo suspeito, é solicitada a realização imediata de uma varredura em todo o computador. A menos que escolha ocultar o aviso da varredura, você receberá lembretes periódicos até executá-la.

Gerenciando arquivos detectados

1. Se o ActiveShield puder limpar o arquivo, você poderá obter mais informações ou ignorar o alerta:
   - Clique em **Obter mais informações** para exibir o nome, o local e o nome do vírus associado ao arquivo detectado.
   - Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e fechá-lo.
2. Se o ActiveShield não puder limpar o arquivo, clique em **Colocar o arquivo detectado em quarentena** para criptografar e isolar temporariamente os arquivos suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada.

   Uma mensagem de confirmação é exibida, solicitando que seja verificada a existência de ameaças no computador. Clique em **Fazer varredura** para concluir o processo de quarentena.
3. Se o ActiveShield não puder colocar o arquivo em quarentena, clique em **Excluir o arquivo detectado** para tentar remover o arquivo.

Gerenciando e-mails detectados

Por padrão, a varredura de e-mails tenta limpar automaticamente o e-mail detectado. Um arquivo de alerta incluído na mensagem de saída informa se o e-mail foi limpo, colocado em quarentena ou excluído.

Gerenciando scripts suspeitos

Quando o ActiveShield detecta um script suspeito, você pode obter mais informações e interromper o script, caso não tenha pretendido iniciá-lo:

- Clique em **Obter mais informações** para exibir o nome, o local e a descrição da atividade associada ao script suspeito.
- Clique em **Interromper este script** para impedir a execução de scripts suspeitos.

Se tiver certeza de que o script é confiável, você pode permitir que ele seja executado:

- Clique em **Permitir este script desta vez** para permitir a execução de todos os scripts contidos em um único arquivo uma vez.
- Clique em **Continuar o que estava fazendo** para ignorar o alerta e deixar o script ser executado.

Gerenciando possíveis worms

Quando o ActiveShield detecta um possível worm, você pode obter mais informações e interromper a atividade de e-mail, caso não tenha pretendido iniciá-la:

- Clique em **Obter mais informações** para exibir a lista de destinatários, a linha de assunto, o corpo da mensagem e uma descrição da atividade suspeita associada à mensagem de e-mail detectada.
- Clique em **Interromper este e-mail** para impedir o envio do e-mail suspeito e excluí-lo da fila de mensagens.

Se tiver certeza de que o e-mail é confiável, clique em **Continuar o que estava fazendo** para ignorar o alerta e permitir o envio do e-mail.

Gerenciando PUPs

Se o ActiveShield detectar e bloquear um programa potencialmente indesejado (PUP), você poderá obter mais informações e remover o programa, caso não pretenda instalá-lo:

- Clique em **Obter mais informações** para exibir o nome, local e a ação recomendada associada ao PUP.
- Clique em **Remover este PUP** para remover o programa, caso não pretenda instalá-lo.

  Uma mensagem de confirmação é exibida.

  - Se você (a) não reconhecer o PUP ou (b) não tiver instalado o PUP como parte de um pacote nem tiver aceitado um acordo de licença associado a esses programas, clique em **OK** para remover o programa usando o método McAfee de remoção.

  - Caso contrário, clique em **Cancelar** para sair do processo de remoção automática. Caso mude de idéia posteriormente, você poderá remover o programa manualmente, usando o programa de desinstalação do fornecedor.
- Clique em **Continuar o que estava fazendo** para ignorar o alerta e bloquear o programa desta vez.

Se você (a) reconhecer o PUP ou (b) tiver instalado o PUP como parte de um pacote ou aceitado um acordo de licença associado a esses programas, poderá permitir sua execução:

- Clique em **Confiar neste PUP** para incluir o programa na lista branca e sempre permitir sua execução no futuro.

  Consulte "*Gerenciando PUPs confiáveis*" para obter detalhes.

Gerenciando PUPs confiáveis

Os programas adicionados à lista de PUPs confiáveis não são detectados pelo McAfee VirusScan.

Se um PUP for detectado e adicionado à lista de PUPs confiáveis, ele poderá ser removido posteriormente, se necessário.

Se a lista de PUPs estiver cheia, será necessário remover alguns itens da lista para poder confiar em outro PUP.

Para remover um programa da lista de PUPs confiáveis:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **PUPs**.
3. Clique em **Editar lista de PUPs confiáveis**, marque a caixa de seleção ao lado do nome do arquivo e clique em **Remover**. Clique em **OK** quando terminar de remover os itens.

Fazendo a varredura manual do computador

O mecanismo de varredura permite procurar vírus e outras ameaças em unidades de disco rígido, disquetes e arquivos e pastas individuais. Ao encontrar um arquivo suspeito, o mecanismo tenta limpá-lo automaticamente, a não ser que seja um programa potencialmente indesejado. Se o mecanismo de varredura não conseguir limpar o vírus, você poderá colocar o arquivo em quarentena ou excluí-lo.

Fazendo a varredura manual de vírus e outras ameaças

Para fazer a varredura do computador:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.

A caixa de diálogo **Fazer varredura** será aberta (Figura 2-8).

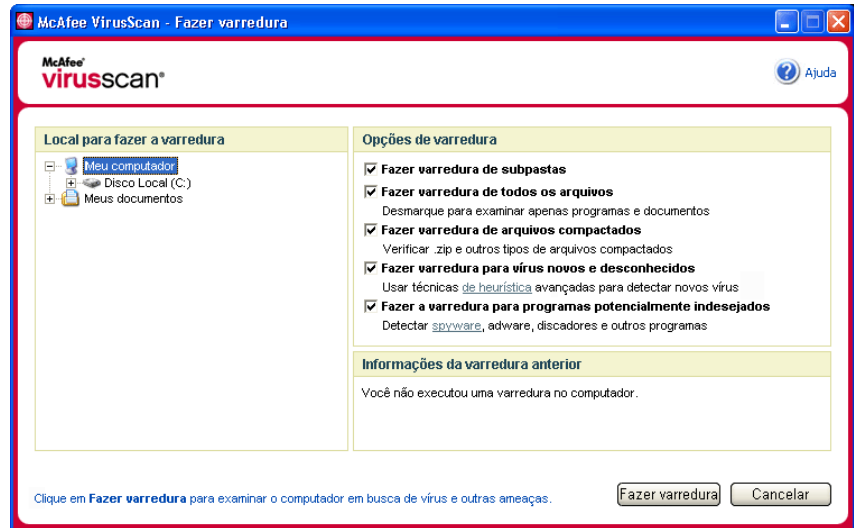



Figura 2-8. Caixa de diálogo Fazer varredura

2 Clique na unidade, pasta ou arquivo em que será feita a varredura.

3 Selecione as suas **Opções de varredura**. Por padrão, todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 2-8):

- **Fazer varredura de subpastas** — use essa opção para fazer a varredura de arquivos contidos nas suas subpastas. Desmarque essa caixa de seleção para permitir a verificação somente dos arquivos que podem ser vistos quando uma pasta ou uma unidade é aberta.

  Exemplo: Os arquivos da Figura 2-9 são os únicos examinados, se você desmarcar a caixa **Fazer varredura de subpastas**. As pastas e seu conteúdo não serão examinados. Para fazer a varredura das pastas e do seu conteúdo, é necessário deixar essa caixa de seleção marcada.

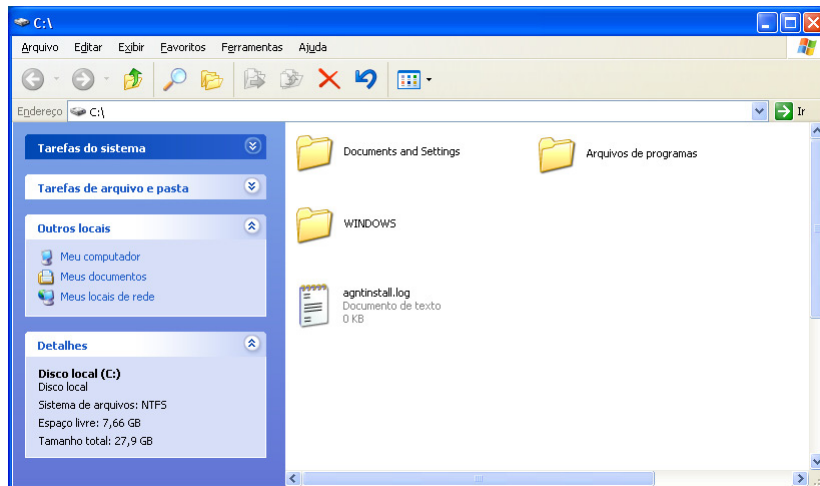



Figura 2-9. Conteúdo do disco local

- **Fazer varredura de todos os arquivos** — use essa opção para permitir a varredura completa de todos os arquivos. Desmarque essa caixa de seleção para diminuir o tempo da varredura e permitir a verificação apenas de documentos e arquivos de programas.
- **Fazer varredura de arquivos compactados** — use esta opção para revelar arquivos ocultos em arquivos .ZIP e outros arquivos compactados. Desmarque essa caixa de seleção para evitar a varredura de arquivos ou arquivos compactados que se encontram em outros arquivos compactados.

  Às vezes, os autores de vírus colocam os vírus em um arquivo .ZIP e, em seguida, inserem esse arquivo .ZIP em outro arquivo .ZIP para tentar burlar os mecanismos antivírus. O mecanismo de varredura pode detectar esses vírus desde que essa opção esteja selecionada.
- **Fazer varredura para vírus novos e desconhecidos** — use essa opção para encontrar os vírus mais recentes para os quais talvez não existam "vacinas". A opção utiliza técnicas avançadas de heurística que tentam estabelecer uma correspondência entre os arquivos e as assinaturas de vírus conhecidos. Ao mesmo tempo, são procurados indícios de vírus desconhecidos nos arquivos.

  Esse método de varredura também examina o arquivo em busca de características que geralmente indicam que ele contém vírus. Isso minimiza a possibilidade de a varredura fornecer indicações falsas. Porém, se uma varredura heurística detectar um vírus, trate-o com o mesmo cuidado destinado a arquivos que você sabe que contêm vírus.

  Essa opção proporciona a varredura mais completa, mas geralmente é mais lenta do que a varredura normal.

- **Fazer varredura para programas potencialmente indesejados** — use esta opção para detectar spyware, adware e outros programas que coletam e transmitem os seus dados pessoais sem a sua permissão.

  NOTA
  Mantenha todas as opções padrão selecionadas para obter a varredura mais completa possível. Esse procedimento fará a varredura de todos os arquivos da unidade ou da pasta selecionada. Portanto, reserve tempo suficiente para que a varredura seja concluída. Quanto maior a unidade de disco rígido e o número de arquivos existentes, mais demorada será a varredura.

4 Clique em **Fazer varredura** para iniciar a varredura dos arquivos.

Quando a varredura for concluída, um resumo informará o número de arquivos examinados e de arquivos detectados, além do número de programas potencialmente indesejados e arquivos detectados que foram limpos automaticamente.

5 Clique em **OK** para fechar o resumo e exibir a lista de todos os arquivos detectados na caixa de diálogo **Fazer varredura** (Figura 2-10).

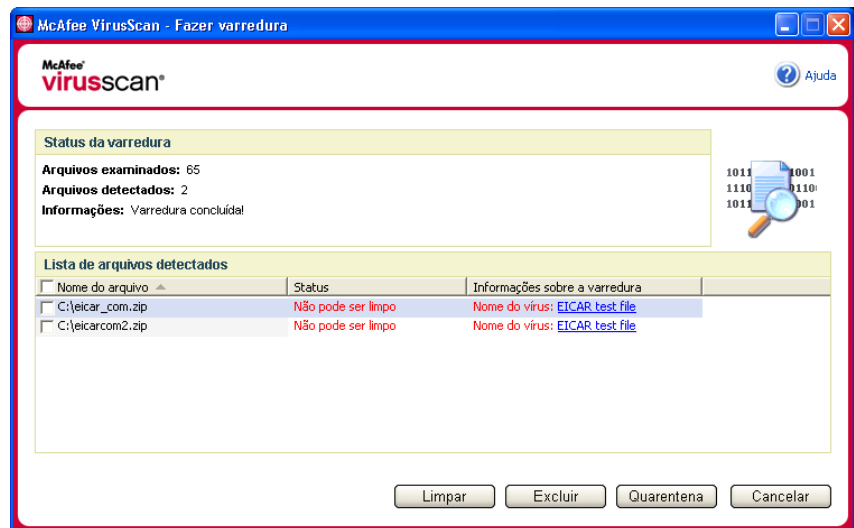



Figura 2-10. Resultados da varredura

NOTA
A varredura considera um arquivo compactado (.ZIP, .CAB, etc.) como um arquivo único na contagem dos **Arquivos examinados**. Além disso, o número de arquivos examinados pode variar se você tiver excluído os arquivos temporários da Internet após a última varredura.

6 Se a varredura não encontrar vírus ou outras ameaças, clique em **Voltar** para selecionar outra pasta ou unidade para a varredura, ou clique em **Fechar** para fechar a caixa de diálogo. Caso contrário, consulte *Entendendo as detecções de ameaças* na página 32.

Fazendo a varredura pelo Windows Explorer

O VirusScan fornece um menu de atalho que permite fazer a varredura de arquivos, pastas ou unidades selecionadas a partir do Windows Explorer, em busca de vírus e outras ameaças.

Para fazer a varredura de arquivos no Windows Explorer:

1 Abra o Windows Explorer.

2 Clique com o botão direito do mouse na unidade, na pasta ou no arquivo em que a varredura será realizada e clique em **Fazer varredura**.

   A caixa de diálogo **Fazer varredura** será exibida e iniciará a varredura dos arquivos. Por padrão, todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 2-8 na página 27).

Fazendo a varredura pelo Microsoft Outlook

O VirusScan fornece um ícone de barra de ferramentas para o Microsoft Outlook 97 ou posterior, que permite verificar a existência de vírus e outras ameaças nos locais selecionados de armazenamento de mensagens e respectivas subpastas, pastas de caixa de correio ou mensagens de e-mail com anexos.

Para fazer a varredura de e-mails no Microsoft Outlook:

1 Abra o Microsoft Outlook.

2 Clique no armazenamento de mensagem, pasta ou mensagem de e-mail que contém um anexo a ser examinado e, em seguida, clique no ícone da barra de ferramentas de varredura de e-mail .

   O mecanismo de varredura de e-mails é aberto e inicia a varredura dos arquivos. Todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 2-8 na página 27).

Fazendo a varredura automática para vírus e outras ameaças

Embora o VirusScan faça a varredura de arquivos quando eles são acessados por você ou por seu computador, você pode programar a varredura automática no Agendador do Windows para fazer a varredura completa em busca de vírus e outras ameaças no computador, em intervalos especificados.

Para programar uma varredura:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta.

2. Clique na guia **Varredura programada** (Figura 2-11 na página 31).

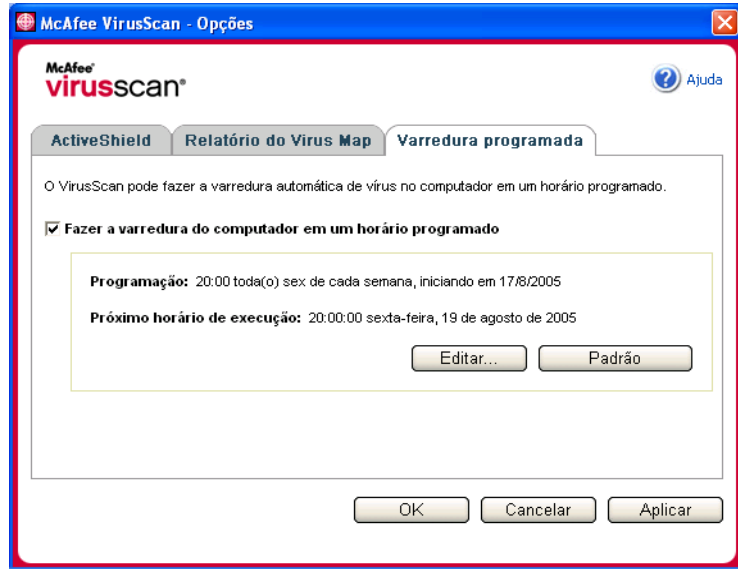



Figura 2-11. Opções de Varredura programada

3. Marque a caixa de seleção **Fazer a varredura do computador em um horário programado** para ativar a varredura automática.

4. Especifique uma programação para a varredura automática:

   - Para aceitar a programação padrão (Todas as sextas-feiras às 20 h), clique em **OK**.

   - Para editar a programação:

     a. Clique em **Editar**.

     b. Selecione a freqüência para fazer a varredura de computador na lista **Programar tarefa** e, em seguida, selecione opções adicionais na área dinâmica abaixo dela:

     Diariamente - Especifique o número de dias entre as varreduras.

     Semanalmente (padrão) - Especifique o número de semanas entre as varreduras, bem como o(s) dia(s) da semana.

Mensalmente - Especifique em qual dia do mês será feita a varredura. Clique em **Selecionar meses** para especificar em quais meses a varredura será feita e, depois, clique em **OK**.

Uma vez - Especifique em qual data a varredura será feita.

NOTA
Não há suporte para as seguintes opções do Agendador do Windows:
Ao inicializar o sistema, **Quando ocioso**, e **Mostrar vários agendamentos**. A última programação com suporte permanecerá ativada até você selecionar uma das opções válidas.

c. Na caixa **Hora de início**, selecione a hora do dia em que a varredura do computador será feita.

d. Para selecionar opções avançadas, clique em **Avançado**.

A caixa de diálogo **Opções de programação avançadas** será aberta.

i. Especifique uma data de início, data de término, duração, hora de término e se deseja interromper a tarefa em uma hora específica caso a varredura ainda esteja sendo executada.

ii. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

5 Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

6 Para retornar à programação padrão, clique em **Padrão**. Caso contrário, clique em **OK**.

Entendendo as detecções de ameaças

Para a maioria dos vírus, cavalos de Tróia e worms, o mecanismo de varredura tenta limpar o arquivo automaticamente. Você pode especificar como gerenciará os arquivos infectados, inclusive se deseja enviá-los aos laboratórios AVERT da McAfee para serem pesquisados. Se o mecanismo de varredura detectar um programa potencialmente indesejado, tente limpá-lo manualmente, colocá-lo em quarentena ou excluí-lo (o envio para a AVERT não está disponível).

Para gerenciar um vírus ou programa potencialmente indesejado:

1 Se um arquivo for exibido na **Lista de arquivos detectados**, clique na caixa de seleção ao lado do arquivo para selecioná-lo.

   NOTA
   Se mais de um arquivo for exibido na lista, você poderá marcar a caixa de seleção exibida na frente da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Você também pode clicar no nome do arquivo na lista **Informações sobre a varredura** para exibir os detalhes da Biblioteca de informações sobre vírus.

2 Se o arquivo for um programa potencialmente indesejado, clique em **Limpar** para tentar limpá-lo.

3 Se o mecanismo de varredura não puder limpar o arquivo, clique em **Quarentena** para criptografar e isolar temporariamente os arquivos suspeitos no diretório de quarentena até que uma ação apropriada possa ser realizada. (Consulte *Gerenciando arquivos em quarentena* na página 33 para obter detalhes).

4 Se o mecanismo de varredura não conseguir limpar o arquivo ou colocá-lo em quarentena, execute uma destas ações:

   - Clique em **Excluir** para remover o arquivo.
   - Clique em **Cancelar** para fechar a caixa de diálogo sem que seja necessária nenhuma outra ação.

Se a varredura não conseguir limpar ou excluir o arquivo detectado, consulte a Biblioteca de informações sobre vírus em http://us.mcafee.com/virusInfo/default.asp para obter instruções sobre a exclusão manual do arquivo.

Se o arquivo detectado não permitir que você utilize a conexão com a Internet ou o computador em geral, tente utilizar um Disco de resgate para iniciar o computador. Em muitos casos, o Disco de resgate pode iniciar o computador que foi desativado pelo arquivo detectado. Consulte *Criando um disco de resgate* na página 35 para obter detalhes.

Para obter mais ajuda, consulte o Atendimento ao cliente da McAfee em http://www.mcafeehelp.com/.

Gerenciando arquivos em quarentena

O recurso Quarentena criptografa e isola temporariamente arquivos suspeitos no diretório de quarentena até que a ação apropriada possa ser executada. Após ser limpo, o arquivo em quarentena pode ser restaurado para o local original.

Para gerenciar um arquivo em quarentena:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Gerenciar arquivos em quarentena**.

Uma lista de arquivos em quarentena é exibida (Figura 2-12).

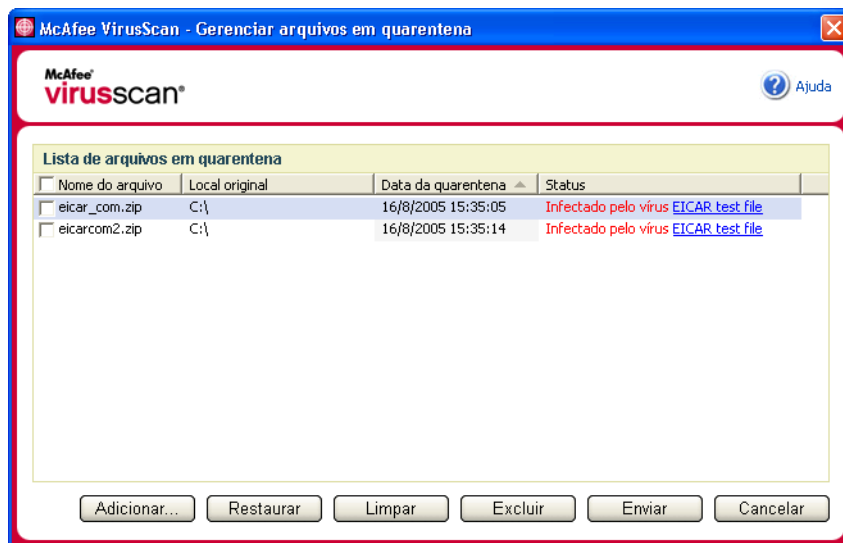



Figura 2-12. Caixa de diálogo Gerenciar arquivos em quarentena

2 Marque as caixas de seleção ao lado dos arquivos a serem limpos.

NOTA
Se mais de um arquivo for exibido na lista, você poderá marcar a caixa de seleção exibida na frente da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Você também pode clicar no nome do vírus na lista **Status** para exibir os detalhes da Biblioteca de informações sobre vírus.

Ou clique em **Adicionar**, selecione um arquivo suspeito para adicionar à lista de quarentena, clique em **Abrir** e selecione-o na lista de quarentena.

3 Clique em **Limpar**.

4 Se o arquivo estiver limpo, clique em **Restaurar** para devolvê-lo para o local original.

5 Se o VirusScan não conseguir limpar o vírus, clique em **Excluir** para remover o arquivo.

6 Se o VirusScan não conseguir limpar ou excluir o arquivo e se ele não for um Programa potencialmente indesejado, você poderá enviá-lo à Equipe de resposta de emergência antivírus da McAfee (AVERT™) para que seja pesquisado:

   a Atualize os arquivos de assinatura de vírus, caso tenham sido recebidos há mais de duas semanas.

b Verifique a sua assinatura.

c Selecione o arquivo e clique em **Enviar** para enviar o arquivo à AVERT.

O VirusScan envia o arquivo em quarentena como um anexo de mensagem de e-mail contendo o seu endereço de e-mail, país, versão de software, sistema operacional, nome e local original do arquivo. O tamanho de envio máximo é um único arquivo de 1,5 MB por dia.

7 Clique em **Cancelar** para fechar a caixa de diálogo sem que seja necessária nenhuma outra ação.

Criando um disco de resgate

O Disco de resgate é um utilitário que cria um disquete inicializável a ser utilizado para iniciar o computador e fazer a varredura de vírus quando um vírus impede a inicialização normal.

NOTA
É necessário estar conectado à Internet para fazer o download da imagem do Disco de resgate. Além disso, o Disco de resgate está disponível somente para computadores com partições de unidades de disco rígido FAT (FAT 16 e FAT 32). Ele é desnecessário para partições NTFS.

Para criar um Disco de resgate:

1 Em um computador não infectado, insira um disquete não infectado na unidade A. Convém usar a opção Fazer varredura para assegurar que não existem vírus no computador e no disquete. (Consulte *Fazendo a varredura manual de vírus e outras ameaças* na página 27 para obter detalhes).

2 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Criar um Disco de resgate**.

A caixa de diálogo **Criar um Disco de resgate** é exibida (Figura 2-13).

Figura 2-13. Caixa de diálogo Criar um Disco de resgate

3 Clique em **Criar** para criar o Disco de resgate.

Ao criar um Disco de resgate pela primeira vez, uma mensagem informa que é preciso fazer o download do arquivo de imagem do Disco de resgate. Clique em **OK** para fazer o download do componente agora ou clique em **Cancelar** para fazê-lo mais tarde.

Uma mensagem de aviso informa que o conteúdo do disquete será perdido.

4 Clique em **Sim** para continuar a criação do Disco de resgate.

O status da criação será exibido na caixa de diálogo **Criar um Disco de resgate**.

5 Quando a mensagem "Disco de resgate criado com êxito" for exibida, clique em **OK** e feche a caixa de diálogo **Criar um Disco de resgate**.

6 Remova o Disco de resgate da unidade, proteja-o contra gravação e armazene-o em um local seguro.

Protegendo um Disco de resgate contra gravação

Para proteger um Disco de resgate contra gravação:

1. Coloque o disquete com o lado do rótulo para baixo (o círculo de metal deve estar visível).
2. Localize a lingüeta de proteção contra gravação. Deslize a lingüeta para que o orifício fique visível.

Usando um Disco de resgate

Para usar um Disco de resgate:

1. Desligue o computador infectado.
2. Insira o Disco de resgate na unidade.
3. Ligue o computador.

   Uma janela cinza com várias opções é exibida.

4. Escolha a opção que atenda melhor às suas necessidades, pressionando as teclas de função (por exemplo, F2, F3).

   NOTA
   Se você não pressionar nenhuma tecla, o Disco de resgate será inicializado automaticamente em 60 segundos.

Atualizando um Disco de resgate

O Disco de resgate deve ser atualizado regularmente. Para atualizar o Disco de resgate, siga as mesmas instruções de criação de um novo Disco de resgate.

Relatando vírus automaticamente

Agora é possível enviar, de forma anônima, informações de controle de vírus para serem incluídas no World Virus Map. Ative automaticamente esse recurso seguro e gratuito durante a instalação do VirusScan (na caixa de diálogo **Relatório do Virus Map**) ou a qualquer momento na guia **Relatório do Virus Map** da caixa de diálogo **Opções do VirusScan**.

Relatando ao World Virus Map

Para relatar automaticamente informações sobre vírus ao World Virus Map:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

A caixa de diálogo **Opções do VirusScan** será aberta.

2 Clique na guia **Relatório do Virus Map** (Figura 2-14).

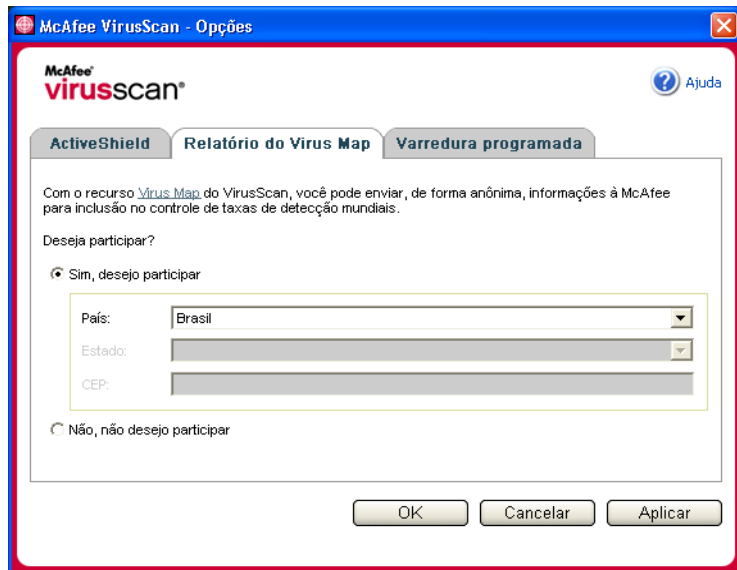



Figura 2-14. - Opções de relatório do Virus Map

3 Aceite a opção padrão **Sim, desejo participar** para enviar anonimamente as informações de vírus para a McAfee, de modo que sejam incluídas no World Virus Map de taxas de detecção mundiais. Caso contrário, selecione **Não, não desejo participar** para evitar o envio de informações.

4 Se estiver nos Estados Unidos, selecione o estado e informe o código de endereçamento postal correspondente ao local onde o seu computador se encontra. Caso contrário, o VirusScan tenta selecionar automaticamente o país em que o seu computador está localizado.

5 Clique em **OK**.

Exibindo o World Virus Map

Sendo participante ou não do World Virus Map, é possível exibir as taxas de detecções mundiais mais recentes usando o ícone da McAfee na bandeja de sistema do Windows.

Para exibir o World Virus Map:

- Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e, em seguida, clique em **World Virus Map**.

  A página da Web do **World Virus Map** é exibida (Figura 2-15).

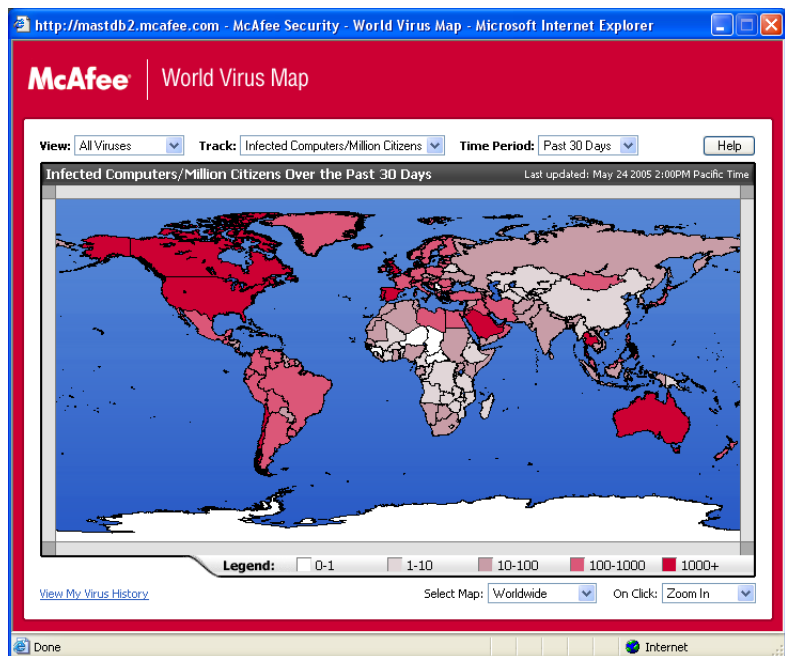



Figura 2-15. World Virus Map

Por padrão, o World Virus Map exibe o número de computadores detectados mundialmente nos últimos 30 dias, além da data em que os dados de relatórios foram atualizados pela última vez. É possível alterar o modo de visualização do mapa para exibir o número de arquivos detectados ou alterar o período para exibir somente os resultados dos últimos 7 dias ou das últimas 24 horas.

A seção **Rastreamento de vírus** lista os totais acumulados do número de arquivos examinados, arquivos detectados e computadores detectados que foram relatados desde a data exibida.

Atualizando o VirusScan

Quando você está conectado à Internet, o VirusScan procura automaticamente atualizações a cada quatro horas. Semanalmente, faz o download automático das atualizações de definições de vírus, instalando-as sem interrupção do trabalho.

Os arquivos de definições de vírus possuem aproximadamente 100 KB e, portanto, causam um impacto mínimo no desempenho do sistema durante o processo de download.

Se ocorrer uma atualização de produto ou epidemia de vírus, um alerta será exibido. Ao receber o alerta, faça a atualização do VirusScan para remover a ameaça de epidemia de vírus.

Verificando atualizações automaticamente

O McAfee SecurityCenter é automaticamente configurado para verificar atualizações de todos os serviços do McAfee a cada quatro horas quando você está conectado à Internet, notificando-o com alertas e sons. Por padrão, o SecurityCenter faz o download e instala automaticamente as atualizações disponíveis.

NOTA
Em alguns casos, é solicitado o reinício do computador para concluir a atualização. Verifique se salvou todo o seu trabalho e fechou todos os aplicativos antes de reiniciar o computador.

Verificando atualizações manualmente

Além de verificar as atualizações automaticamente a cada quatro horas quando se está conectado à Internet, também é possível verificar manualmente as atualizações a qualquer momento.

Para verificar as atualizações do VirusScan manualmente:

1. Verifique se o computador está conectado à Internet.
2. Clique com o botão direito do mouse no ícone da McAfee e, em seguida, clique em **Atualizações**.

   A caixa de diálogo **Atualizações do SecurityCenter** será aberta.

3 Clique em **Verificar agora**.

Se houver uma atualização, a caixa de diálogo **Atualizações do VirusScan** será aberta (Figura 2-16 na página 40). Clique em **Atualizar** para continuar.

Se nenhuma atualização estiver disponível, será aberta uma caixa de diálogo informando que o VirusScan está atualizado. Clique em **OK** para fechar a caixa de diálogo.

Figura 2-16. Caixa de diálogo Atualizações

4 Se solicitado, efetue logon no site da Web. O **Assistente de atualização** instala a atualização automaticamente.

5 Clique em **Concluir** quando a instalação da atualização estiver concluída.

NOTA
Em alguns casos, é solicitado o reinício do computador para concluir a atualização. Verifique se salvou todo o seu trabalho e fechou todos os aplicativos antes de reiniciar o computador.

Índice

A

C

D

E

F